ABSTRACT FOR JP2002-540482

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/00 | A2

(11) International Publication Number: WO 00/59153

(43) International Publication Date: 5 October 2000 (05.10.00)

(21) International Application Number: PCT/US00/06916

(22) International Filing Date: 16 March 2000 (16.03.00)

(30) Priority Data:
09/283,096 31 March 1999 (31.03.99) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

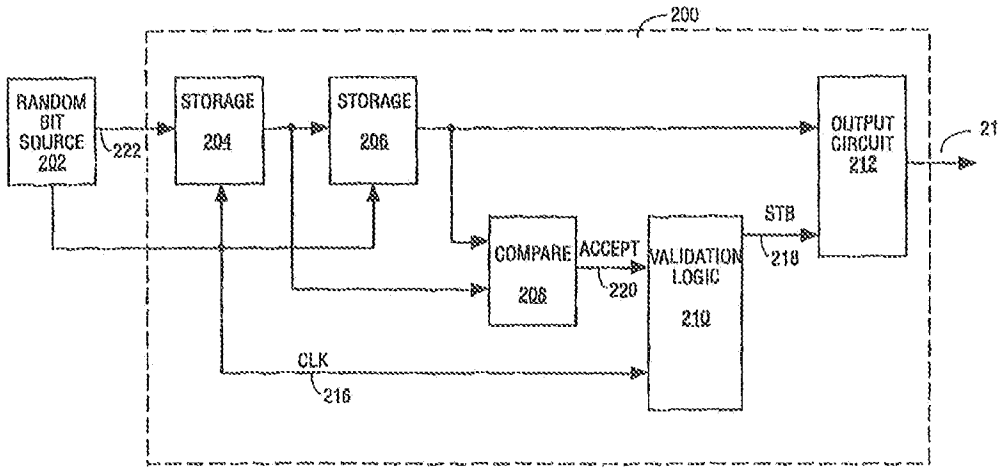
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: WELLS, Steven, E. [US/US]; 4236 Weathervane Court, El Dorado Hills, CA 95762 (US). WARD, David, A. [US/US]; 2808 Honeysuckle Way, Sacramento, CA 95826 (US).

(74) Agents: MILLIKEN, Darren, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: DUTY CYCLE CORRECTOR FOR A RANDOM NUMBER GENERATOR



(57) Abstract

A method and apparatus for producing a corrected bit stream from a random bit stream output by a random bit source. Sequential pairs of bits in the random bit stream are compared. If both bits in a pair of bits are identical, the output bits are discarded. If both bits in a pair of bits are different, one bit of the pair of bits is taken as the output bit.

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号
特表2002－540482
（P2002－540482A）
(43)公表日　平成14年11月26日(2002.11.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ	

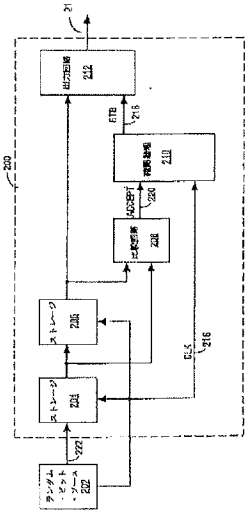
審査請求　未請求　予備審査請求　有　（全 43 頁）

(21)出願番号　特願2000－608542(P2000－608542)
(86)(22)出願日　平成12年３月16日(2000.3.16)
(85)翻訳文提出日　平成13年９月28日(2001.9.28)
(86)国際出願番号　ＰＣＴ／ＵＳ００／０６９１６
(87)国際公開番号　ＷＯ００／５９１５３
(87)国際公開日　平成12年10月５日(2000.10.5)
(31)優先権主張番号　０９／２８３，０９６
(32)優先日　平成11年３月31日(1999.3.31)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　インテル・コーポレーション
アメリカ合衆国　95052　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・2200
(72)発明者　ウエルズ・スティーブン・イー
アメリカ合衆国・95762・カリフォルニア州・エル　ドラド　ヒルズ・ウェザーベイン　コート・4236
(72)発明者　ワード，デイビッド・エイ
アメリカ合衆国・95826・カリフォルニア州・サクラメント・ハニーサックル　ウェイ・2808
(74)代理人　弁理士　山川　政樹
Ｆターム(参考)　5J104 FA00

(54)【発明の名称】　乱数発生器用デューティ・サイクル修正器

(57)【要約】
ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから、修正後のビット・ストリームを生成する方法および装置。それにおいては、ランダム・ビット・ストリーム内のビットの連続するペアが比較される。ビットのペアを構成するの２つのビットがまったく等しい場合には、出力されたビットが破棄される。ビットのペアを構成する２つのビットが互いに異なる場合には、そのビットのペアの一方のビットを出力ビットとして採用する。



【特許請求の範囲】

【請求項１】　ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから修正後のビット・ストリームを生成する方法において：

前記ランダム・ビット・ストリーム内のペアとなるビットを互いに比較するステップ；

前記ビットが等しい場合には前記ペアとなるビットを破棄するステップ；

前記ランダム・ビット・ストリーム内のもう１つのビットを破棄するステップ；および、

前記ペアとなるビットが等しくない場合には前記ペアとなるビットのうちの１つを出力するステップ；

を包含することを特徴とする方法。

【請求項２】　前記もう１つのビットを破棄するステップは、前記比較するステップに先行して起こることを特徴とする前記請求項１記載の方法。

【請求項３】　前記もう１つのビットを破棄するステップは、前記ペアとなるビットを破棄するステップに後続して起こることを特徴とする前記請求項２記載の方法。

【請求項４】　前記ペアとなるビットのうちの１つを出力するステップは、前記ペアとなるビットのうちの最初のビットを出力するステップを構成することを特徴とする前記請求項１記載の方法。

【請求項５】　前記ペアとなるビットのうちの１つを出力するステップは、前記ペアとなるビットのうちの２番目のビットを出力するステップを構成することを特徴とする前記請求項１記載の方法。

【請求項６】　さらに、直列結合されたラッチのペア内に前記ペアとなるビットを同期させてラッチするステップを含むことを特徴とする前記請求項１記載の方法。

【請求項７】　さらに：

その後に続く別のペアとなるビットを比較するステップ；および、

前記ビットを比較した２つのペアの間ある、前記ランダム・ビット・ストリーム内のビットを破棄するステップ；

を包含することを特徴とする前記請求項１記載の方法。

【請求項８】　さらに、前記ペアとなるビットが等しいか等しくないかによらず、前記ランダム・ビット・ストリーム内の前記もう１つのビットを破棄するステップを含むことを特徴とする前記請求項１記載の方法。

【請求項９】　ランダム・ビット・ソースから一様なデューティ・サイクルの出力を生成する前記方法は、ネットワーク内の複数のコンピュータ間における安全な通信のための暗号システムに使用されるランダムなバイナリ数を生成するように動作し得る乱数発生器に使用されることを特徴とする前記請求項２記載の方法。

【請求項１０】　ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから修正後のビット・ストリームを生成するためのデューティ・サイクル修正器回路において：

入力および出力を有し、前記入力が前記ランダム・ビット・ソースからランダム・ビット・ストリームを受け取るべく結合された第１のストレージ回路；

入力および出力を有し、前記入力が前記第１のストレージ回路の出力に結合された第２のストレージ回路；

前記第１のストレージ回路の出力および前記第２のストレージ回路の出力に結合された比較回路；および、

前記比較回路の出力を受け取る第１の入力、および周期的な信号を受け取る第２の入力を有する確認論理であって、前記第１のストレージ回路または前記第２のストレージ回路内にストアされたデータが、修正後のビット・ストリーム内のビットであるとき、それを示す信号を出力する確認論理；

を備えることを特徴とするデューティ・サイクル修正器回路。

【請求項１１】　前記第１のストレージ回路および前記第２のストレージ回路は、ラッチを包含することを特徴とする前記請求項１０記載のデューティ・サイクル修正器回路。

【請求項１２】　前記比較回路は、エクスクルーシブーオア・ゲートを包含することを特徴とする前記請求項１０記載のデューティ・サイクル修正器回路。

【請求項１３】　さらに、前記確認論理によって出力された前記信号を受け

取るべく結合され、かつ前記第１または第２のストレージ回路にストアされたビットを受け取るべく結合された出力回路であって、前記ビット・ストリーム内の修正後のビットを出力する出力回路を備えることを特徴とする前記請求項１０記載のデューティ・サイクル修正器回路。

【請求項１４】　前記出力回路はストレージ回路を包含することを特徴とする前記請求項１３記載のデューティ・サイクル修正器回路。

【請求項１５】　前記確認論理は：

前記ランダム・ビット・ソースのクロック出力に結合されたトランスペアレント・ラッチ；および、

前記トランスペアレント・ラッチの出力に結合された第１の入力、および前記比較回路の出力に結合された第２の入力を有するアンド・ゲート；

を包含することを特徴とする前記請求項１０記載のデューティ・サイクル修正器回路。

【請求項１６】　前記確認論理は：

前記ランダム・ビット・ソースのクロック出力に結合されたモジュロＸカウンタであって、Ｘは１より大きい整数とするモジュロＸカウンタ；および、

前記モジュロＸカウンタの出力に結合された第１の入力、および前記比較回路の出力に結合された第２の入力を有するアンド・ゲート；

を包含することを特徴とする前記請求項１０記載のデューティ・サイクル修正器回路。

【請求項１７】　コンピュータとネットワーク・メディアの間においてメッセージの送信および受信を行うべく動作し得るネットワーク・インターフェース・デバイス；および、

前記コンピュータから送信されるメッセージの符号化および復号化を行うべく動作し得る暗号化回路／解読回路であって、ランダム・ビット・ストリームを生成するように動作し得る乱数発生器を有し、それにおいて前記乱数発生器は：

未修正ビット・ストリームを出力するように動作し得る乱数発生器；および、

デューティ・サイクル修正器回路であって：

入力および出力を有し、前記入力が前記ランダム・ビット・ソースから前記未

修正ランダム・ビット・ストリームを受け取るべく結合された第１のストレージ回路；

入力および出力を有し、前記入力が前記第１のストレージ回路の出力に結合された第２のストレージ回路；

前記第１のストレージ回路の出力および前記第２のストレージ回路の出力に結合された比較回路；および、

前記比較回路の出力を受け取る第１の入力、および周期的な信号を受け取る第２の入力を有する確認論理であって、前記第１のストレージ回路または前記第２のストレージ回路内にストアされたデータが、修正後のビット・ストリーム内のビットであるとき、それを示す信号を出力する確認論理；

を包含するデューティ・サイクル修正器回路；

を備えるものとする暗号化回路／解読回路；

を備えることを特徴とするコンピュータ。

【請求項１８】　前記暗号化回路／解読回路は、さらに暗号ベースの暗号化方法を使用する前記コンピュータによって送信され、受信されるメッセージの符号化および復号化を行うべく動作し得ることを特徴とする前記請求項１７記載のコンピュータ。

【請求項１９】　前記暗号ベースの暗号化方法は、単一キーシステムであることを特徴とする前記請求項１９記載のコンピュータ。

【請求項２０】　前記暗号ベースの暗号化方法は、公開キー／秘密キーシステムであることを特徴とする前記請求項１９記載のコンピュータ。

【発明の詳細な説明】

【０００１】

（技術分野）

本発明は、全体的にコンピュータ・セキュリティに関し、より詳細に述べれば、乱数発生器におけるほぼ一様なデューティ・サイクルの発生に関する。

【０００２】

（発明の背景）

乱数発生回路は、各種の電子応用において使用されている。乱数発生器に関する重要な応用の１つに、メッセージ・データの暗号化と解読が行なわれるコンピュータ・セキュリティの分野におけるものがある。暗号システムは、データを、符号化したメッセージに変える変換を含み、それが送信されたとき、意図された受取人だけがそれを復号することができる。もっとも一般的な暗号テクニックにおいては、暗号（キー）が使用され、送り側はそれを用いてメッセージを符号化し、受け側はそれを用いて当該符号化されたメッセージを復号する。広く知られた暗号システムには、メッセージの符号化および復号化に単一のキーを使用する方法と、メッセージの符号化とその復号化にそれぞれ別のキーを使用する方法がある。

【０００３】

メッセージの符号化および復号化に使用されるキーは、基本的にバイナリ・データ・パターンであり、それに照らしてメッセージの処理、すなわちフィルタリングが行なわれる。効果的な暗号システムは、充分に大きなビット数を有し、再生がほとんど不可能なキーの使用を必要とする。さらに、キーを構成するデータ・パターンは、そのキーによって符号化が行なわれたメッセージ内において、それらのパターンないしはパターン群を予測不能にできる充分なランダム性を有していなければならない。したがって効果的な暗号システムには、メッセージ内のバイナリ・データが完全に予測不能な態様で変換されることを保証するように、質の高い乱数発生器を使用する必要がある。一般に、暗号スキームにおけるランダム性の欠如は、符号化済みデータと未符号化データの間に、ある種の相関をもたらす。その後、この相関を使用し、符号化済みメッセージに基づいて試行錯誤

を繰り返し、可能性のある出力パターンの予測といったテクニックを通じて、コードの盗み出しが可能になる。

【０００４】

バイナリ乱数に望ましい特徴は、純粋にランダムな順序において「０」と「１」のビットが出力されることである。すなわち、あらゆる時点において出力ビットの値が完全に予測不能となることである。乱数発生器の出力のデューティ・サイクルは、無限の標本サイズにわたって約５０パーセントとなり、出力が論理ロー（「０」）になる確率と、出力が論理ハイ（「１」）になる確率が等しくなることが望ましい。また、乱数発生器によって示される任意ビットと他のビットの間の相関が低く（たとえば、約ゼロの相関）、出力ビットの間のフーリエ分布が平坦になることが望ましい。

【０００５】

しかしながら、現在知られている乱数発生器は、統計的に有意な標本サイズにわたって「０」の数と「１」の数が等しくならない傾向にある。従来技術の乱数発生器が一様でないデューティ・サイクルとなる共通の理由としては、禁止されたセットアップ／ホールドタイムの間にデータがラッチされたとき、一般に、乱数発生器を構成するラッチが２つの状態のうちの一方に偏ることが挙げられる。乱数発生器におけるデューティ・サイクルの変動を抑える現在の一般的な方法は、ランダム・ビット・ソースの出力段におけるリニア・フィードバック・シフト・レジスタ（ＬＦＳＲ）の使用が関連する。

【０００６】

図１は、従来技術における乱数発生器の一例を示しており、ランダム・ビット・ソース１０２の出力と結合されるリニア・フィードバック・シフト・レジスタ１０４を使用する。ＬＦＳＲ　１０４は、多数のラッチ１０５とゲート１０６を含み、それを通じてランダム・ビット・ソース１０２からの出力ビットが伝播される。出力ビットの状態は、ゲート１０６によってランダムに反転され、ビットの順序がさらに、ラッチ１０５を通るビットのフィードバックを介して撹乱される。

【０００７】

概して、図１に示したようなリニア・フィードバック・シフト・レジスタは、特定の不利益を有し、しかも典型的なランダム・ビット・ソースによってもたらされる一様でないデューティ・サイクル特性の完全な修正が得られない。ＬＦＳＲ　１０４によって示されるように、通常、ＬＦＳＲ自体が複数のラッチとゲートを包含している。これらのラッチとゲートは、ランダム・ビット・ソース１０２内のラッチの場合に同じく、特定の状況下において「０」または「１」のラッチへ偏る傾向にある。つまり、通常のＬＦＳＲ自体が「１」と「０」の一様なデューティ・サイクルを生成せず、そのためランダム・ビット・ソースにおけるデューティ・サイクルの変動を完全には修正し得ない。

【０００８】

それ以外にもリニア・フィードバック・シフト・レジスタは、多数のラッチとゲートを必要とするという不利益がある。たとえば、図１に示したような３２ビットのＬＦＳＲであれば、３２個のＤタイプのラッチが必要になるだけでなく、多数の組み合わせゲートが必要になる。このことは、この種のＬＦＳＲを使用する乱数発生器のために必要となるシリコン面積を格段に増加させることになる。

【０００９】

（発明の要約）

ここでは、ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから、修正後のビット・ストリームを生成する方法および装置を開示する。それにおいては、ランダム・ビット・ストリーム内のビットの連続するペアが比較される。ビットのペアを構成する２つのビットがまったく等しい場合には、出力されたビットが破棄される。ビットのペアを構成する２つのビットが互いに異なる場合には、そのビットのペアの一方のビットを出力ビットとして採用する。

【００１０】

このほかの本発明の特徴ならびに利点は、添付の図面および以下の詳細な説明から逐次明らかなものとなろう。

【００１１】

なお、添付図面には、限定の意味ではなく、例示のための手段として本発明が

示されており、それらにおいては、類似の要素に類似の参照番号が用いられている。

【００１２】

（詳細な説明）

乱数発生器内で使用するデューティ・サイクル修正器を説明する。一実施形態においては、このデューティ・サイクル修正器によって、ランダム・ビット・ソースから出力されたビットの連続するペアが処理される。ビットのペアを構成する２つのビットがまったく等しい場合には、デューティ・サイクル修正器によってそのビットのペアが破棄されるか、あるいは出力されない。ビットのペアを構成する２つのビットが互いに異なる場合には、デューティ・サイクル修正器によってビット・ペア内のビットの一方が出力される。

【００１３】

本発明の実施形態の利点として意図されていることは、ランダム・ビット・ソースの出力に関してほぼ一様なデューティ・サイクルを生成する回路を提供することである。さらに、集積回路デバイス内に実装された場合に、必要とするシリコン面積が小さい乱数発生器を提供することも本発明の実施形態の利点として意図されている。

【００１４】

ここで、ランダム・ビット・ソースは、ランダムと推定される順序でバイナリ・ディジット系列を出力するディジタル回路であることを思い出されたい。理想的なランダム・ビット・ソースにおいては、所定の出力ビットが「０」となる確率が、それが「１」となる確率に等しい。つまり、ランダム・ビット・ソースの出力波形のデューティ・サイクルは、統計的に有意な標本サイズにわたって一様に５０パーセントとなる。しかしながら、ほとんどのランダム・ビット・ソースは、禁止されたホールドタイムまたはセットアップタイムの間にデータがラッチされると、ランダム・ビット・ソース内のラッチならびにゲートが特定の論理・レベルをラッチするという傾向に起因したデューティ・サイクルの変動を呈する。

【００１５】

ランダム・ビット・ソースによって特定時に所定のビットが出力される確率は、一定の数学的関係によって表すことができる。たとえば、出力が「０」になる確率（Ｐ（０））をｐとすれば、出力が「１」となる確率（Ｐ（１））は１－ｐで表される。すなわち、

「０」を生成する確率：Ｐ（０）＝ｐ

「１」を生成する確率：Ｐ（１）＝１－ｐ

である。理想的なランダム・ビット・ソースにおいては、ｐが５０パーセントになる。逆に、理想的でないランダム・ビット・ソースの場合は、ｐが５０パーセントより実質的に大きくなるか、あるいはそれより小さくなる。

【００１６】

ランダム・ビット・ソースの連続する出力をペアとして考えると、この確率は次のようになる。

「０」「０」を生成する確率：Ｐ（００）＝Ｐ（０）Ｐ（０）＝p^2

「０」「１」を生成する確率：Ｐ（０１）＝Ｐ（０）Ｐ（１）＝ｐ（１－ｐ）

「１」「０」を生成する確率：Ｐ（１０）＝Ｐ（１）Ｐ（０）＝（１－ｐ）ｐ

「１」「１」を生成する確率：Ｐ（１１）＝Ｐ（１）Ｐ（１）＝$(1-p)^2$

【００１７】

数学的に、「０」「１」の出力ペアと「１」「０」の出力ペアが生成される確率は、上記の確率の式からもわかるように、互いに等しい。つまり、ｐ（１－ｐ）＝（１－ｐ）ｐであり、したがってＰ（０１）＝Ｐ（１０）である。

【００１８】

この性質は、ランダム・ビット・ソースが「１」を生成する確率、または「０」を生成する確率とは無関係に、与えられた任意の出力に関して真となる。したがって、特定のランダム・ビット・ソースについて、ｐが５０パーセントとならない場合であっても、そのランダム・ビット・ソースが「０－１」の出力ペアを生成する確率は、それが「１－０」の出力ペアを生成する確率に等しい。本発明の一実施形態においては、この原理を用いて、一様でないデューティ・サイクルを呈し、かつ所定の出力ビット・ストリーム内の「０」と「１」の分布が一様でないランダム・ビット・ソースの出力を訂正する。

【００１９】

本発明の１つの方法においては、デューティ・サイクル修正器がランダム・ビット・ソースから出力されたペアとなるビットを処理して、修正した、実質的にデューティ・サイクルが一様なビット・ストリームを決定する。一実施形態においては、ビットのペアを構成するビットがともに等しいときには、デューティ・サイクル修正器によってそのペアが破棄され、修正後のビット・ストリームの一部として出力されない。つまり、出力ビットのペアを構成するビットがともに「０」であれば、そのペアが破棄される。それと同様に、出力ビットのペアを構成するビットがともに「１」であれば、そのペアが破棄される。しかしながら、出力ビットのペアを構成するビットが互いに異なれば、デューティ・サイクル修正器により、そのペアの一方のビットが修正後のビット・ストリームの１つのビットとして出力される。一実施形態においては、デューティ・サイクル修正器が異なるビットからなるペア内の最初のビットを修正後のビットとして出力する。したがって、この実施形態においては、出力ペアが「０－１」であれば修正後のビットが「０」にセットされ；出力ペアが「１－０」であれば修正後のビットが「１」にセットされる。各種のペアの場合に対応する修正後のビット値は、次の関係を用いて表すことができる。

Ｐ（００）＝Ｐ（０）Ｐ（０）＝p^2　　破棄される

Ｐ（０１）＝Ｐ（０）Ｐ（１）＝ｐ（１－ｐ）　論理「０」が出力される

Ｐ（１０）＝Ｐ（１）Ｐ（０）＝（１－ｐ）ｐ　論理「１」が出力される

Ｐ（１１）＝Ｐ（１）Ｐ（１）＝$(1-p)^2$　　破棄される

【００２０】

変形実施形態においては、デューティ・サイクル修正器が異なるビットからなるペア内の２番目のビットを修正後のビットとして出力する。つまり、この実施形態においては、出力ペアが「０－１」であれば修正後のビットが「１」にセットされ；出力ペアが「１－０」であれば修正後のビットが「０」にセットされる。したがって、この変形実施形態における各種のペアの場合に対応する修正後のビット値は、次の関係を用いて表すことができる。

Ｐ（００）＝Ｐ（０）Ｐ（０）＝p^2　　破棄される

Ｐ（０１）＝Ｐ（０）Ｐ（１）＝ｐ（１－ｐ）　論理「１」が出力される
Ｐ（１０）＝Ｐ（１）Ｐ（０）＝（１－ｐ）ｐ　論理「０」が出力される
Ｐ（１１）＝Ｐ（１）Ｐ（１）＝$(1-p)^2$　破棄される

【００２１】

図２は、上記の実施形態を具体化したデューティ・サイクル修正器２００の一実施形態を示しており、それにおいては、ランダム・ビット・ソース２０２の出力から実質的に一様なビット・ストリームが生成され、しかも従来のＬＦＳＲ回路より使用されているゲート数が少ない。ランダム・ビット・ソース２０２は、信号ライン２２２上にランダムなビットのストリームを出力するものであれば、任意のランダム・ビット・ソースとすることができる。本発明の一実施形態においては、ランダム・ビット・ソース２０２が、高速発振信号を周期的にラッチするランダムに変化させた低速クロック信号を使用するラッチ回路として実装される。ランダム・ビット・ソースのラッチから出力されるビットの値は、低速信号によってラッチされたときの高速信号の電圧レベルに依存する。またランダム・ビット・ソース２０２は、この分野において一般に知られているように、クロック信号またはストローブ信号ＣＬＫを生成して信号ライン２１６上に供給する。

【００２２】

デューティ・サイクル修正器２００は、ストレージ・エレメント２０４と２０６、比較回路２０８、確認論理２１０、および出力回路２１２を含んでいる。ストレージ回路２０４と２０６は、ランダム・ビット・ソース２０２から出力されたランダム・ビット・ストリーム内の連続するビットをペアとして、比較回路２０８による比較のためにストアする。ＣＬＫの第１のクロック・サイクルにおいて、ペアとなるビットの最初のビットがストレージ回路２０４にストアされる。この最初のビットは、続くクロック・サイクルにおいてストレージ回路２０６にストアされ、ストレージ回路２０４には、そのときランダム・ビット・ソース２０２から出力された次のビットがストアされる。ストレージ回路２０４と２０６は、ラッチ、レジスタ、揮発性もしくは不揮発性メモリ・セル、およびその他の等価物を含めた任意のタイプのストレージ・エレメントとすることができる。

【００２３】

ストレージ回路２０４と２０６にストアされたビットは、比較回路２０８によって比較される。この比較回路２０８は、エクスクルーシブーオア・ゲートもしくはコンパレータといった任意のタイプの比較回路とすることができる。２つのビットが等しいときには、比較回路２０８が、信号ライン２２０上の信号を論理ハイの状態にセットしてＡＣＣＥＰＴ（アクセプト）をアサートする。２つのビットが等しくないときには、比較回路２０８が、その信号を論理ローの状態にセットしてＡＣＣＥＰＴ（アクセプト）のアサートを解く。つまり、ＡＣＣＥＰＴ（アクセプト）信号は、ランダム・ビット・ソースから出力されるペアとなるビットが、デューティ・サイクル修正器２００によって出力されるビット・ストリーム内の修正後のビットとなり得るか否かを示すことになる。

【００２４】

ＡＣＣＥＰＴ（アクセプト）信号は、ＣＬＫとともに確認論理２１０に渡される。比較回路２０８は、ストレージ回路２０４と２０６内の連続する２つのビットが互いに異なるとき、ＡＣＣＥＰＴ（アクセプト）をアサートする。しかしながら、デューティ・サイクル修正器２００が一様なデューティ・サイクルの出力ストリームを生成するためには、ランダム・ビット・ソース２０２から出力されるビットをオーバーラップさせることなく比較する方が好ましい。その機能を具体化している部分が確認論理２１０である。確認論理２１０は、ＡＣＣＥＰＴ（アクセプト）がアサートされ、かつ望ましいビットのペアがストレージ回路２０４と２０６にストアされているとき、信号ライン２１８上の信号を論理ハイの状態にセットしてストローブ信号ＳＴＢをアサートする。ＳＴＢがアサートされると、出力回路２１２がストレージ回路２０６内のビットをストアする。出力回路２１２は、レジスタ、ラッチ、１ないしは複数の揮発性もしくは不揮発性メモリ・エレメント、アンド・ゲート、あるいはその他の論理を含めて任意のストレージ・エレメントとすることができる。出力回路２１２によってストアされたビットは、ストレージ回路２０４と２０６内にストアされたビットに対応する修正後のビットとして信号ライン２１４に出力される。

【００２５】

変形実施形態に関しては、ストレージ回路２０６の出力に代えてストレージ回

路２０４の出力を出力回路２１２に渡すことができる。その実施形態の場合、ＳＴＢがアサートされると出力回路２１２がストレージ回路２０４内のビットをストアし、このビットをストレージ回路２０４と２０６内にストアされたビットに対応する修正後のビットとして出力する。

【００２６】

図３は、デューティ・サイクル修正器２００の一実施形態であるデューティ・サイクル修正器３００を示している。デューティ・サイクル修正器３００は、ストレージ回路２０４と２０６のそれぞれ一実施形態であるラッチ３０４および３０６；比較回路２１０の一実施形態であるエクスクルーシブーオア・ゲート３１０；確認論理２１０の一実施形態であるトランスペアレント・ラッチ３０８およびアンド・ゲート３０９の組み合わせ；および出力回路２１２の一実施形態であるラッチ３１２を含んでいる。

【００２７】

ラッチ３０４および３０６は、ランダム・ビット・ソース２０２から出力された連続するビットをペアとして、エクスクルーシブーオア・ゲート３１０による比較のためにストアする。ペアとなるビットの最初のビットが、ＣＬＫによってラッチ３０４内にラッチされる。ＣＬＫの次のクロック・パルスでは、この最初のビットがラッチ３０６にラッチされ、ランダム・ビット・ソース２０２から出力された次のビットがラッチ３０４内にラッチされる。ビットのペアを構成する２つのビットが等しければ、エクスクルーシブーオア・ゲート３１０がＡＣＣＥＰＴ（アクセプト）のアサートを行わずに「０」を出力し；ビットのペアを構成する２つのビットが互いに異なれば、エクスクルーシブーオア・ゲート３１０が「１」を出力してＡＣＣＥＰＴ（アクセプト）をアサートする。

【００２８】

トランスペアレント・ラッチ３０８は、ランダム・ビット・ソース３０２からのＣＬＫをラッチし、ＡＣＣＥＰＴ（アクセプト）がアサートされ、かつラッチ３０４および３０６にオーバーラップのないビットのペアがストアされているときにＳＴＢがアサートされるようにアンド・ゲート３０９をクロックする。ＳＴＢがアサートされると、ラッチ３１２がラッチ３０６から出力されたビットを、

信号ライン２１４上に出力する修正後のビットとしてラッチする。別の実施形態においては、ラッチ３０４の出力をラッチ３１２に供給することができる。このビットを、ラッチ３１２によりＳＴＢに応答してラッチすればよい。

【００２９】

図４は、デューティ・サイクル修正器３００の動作を示したフローチャートである。ステップ４００において、ラッチ３０４および３０６がランダム・ビット・ソース２０２から最初のペアとなるビットをラッチするが、そのうちの最初のビットはラッチ３０６にストアされ、２番目のビットはラッチ３０４にストアされる。ステップ４０２においては、エクスクルーシブーオア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを決定する。ペアを構成する２つのビットが等しいときには、ステップ２０４において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ２０４においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。しかしながら、ステップ４０２において２つのビットが互いに異なると判断されると、ステップ４０６においてペア内の最初のビットが出力として獲得される。

【００３０】

ステップ４０８においては、続くオーバーラップするペアとなるビットがランダム・ビット・ソース２０２から取り込まれ、その後プロセスがステップ４０２から繰り返される。このプロセスは、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。ペアを構成しない乱数源からの出力ビットは、処理不可能であり、したがって破棄される。ここでは、ペアを構成する最初のビットがラッチ３０６から修正後のビットとして供給されているが、別の方法においては、修正後のビットとして、ペアを構成する２番目のビットをラッチ３０４から供給できることに注意する必要がある。

【００３１】

図５は、デューティ・サイクル修正器３００の動作をさらに別の形で説明している。図５を参照すると、２番目のペアとなるビット（ビット２および３）およ

び３番目のペアとなるビット（ビット４および５）は修正後のビットを生成するが、最初のペアとなるビット（ビット０および１）および４番目のペアとなるビット（ビット６および７）からは生成されないことがわかる。

【００３２】

ランダム・ビット・ソース２０２は、ラッチ、論理ゲート、およびその他の回路エレメントの特性に起因して、連続的に生成されたビットの間に１次の自己相関を有するビットを出力することがある。つまり、図２および３に示したような上記のデューティ・サイクル修正器が実質的に一様なデューティ・サイクルを有するランダム・ビット・パターンを実質的に出力できる場合であっても、ランダム・ビット・ソースによって出力されるビット間の自己相関が低くないとデューティ・サイクル修正器の出力が一様なデューティ・サイクルに近づく可能性が高くならない。言い換えれば、ランダム・ビット・ストリーム内のビットが互いに相関を有していない場合においては、デューティ・サイクル修正器の出力が一様なデューティ・サイクルに近づく可能性が高くなる。

【００３３】

図５に示されるように、図３に示したデューティ・サイクル修正器３００は、ビットの連続するペアに対してデューティ・サイクル修正器３００が作用することから、ランダム・ビット・ソース２０２によって出力されたランダム・ビット・ストリーム内のビット間における１次の自己相関による影響を受けることがあり得る。図６は、別の実施形態、すなわちランダム・ビット・ソース２０２によって出力されるビットのペアの間における１次の自己相関の影響を軽減するデューティ・サイクル修正器６００を示している。このデューティ・サイクル修正器６００は、修正後のビットを生成したビットのペアが検出されるごとに、ランダム・ビット・ソース２０２から出力されるビットを１つ破棄することによって１次の自己相関の影響を軽減する。

【００３４】

デューティ・サイクル修正器６００は、デューティ・サイクル修正器３００に類似であるが、確認論理のトランスペアレント・ラッチ３０８がモジュロ２カウンタ６０２に置き換えられている点が異なる。デューティ・サイクル修正器６０

０の動作を図７に示す。ステップ７００においては、モジュロ２カウンタ６０２のカウント「０」と「１」に応答して、ラッチ３０４および３０６がランダム・ビット・ソース２０２からの最初のペアとなるビットをラッチする。ステップ７０２においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを決定する。ペアを構成する２つのビットが等しいときには、ステップ７０４において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ７０４においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。しかし、ステップ７０２において２つのビットが互いに異なると判断されると、ステップ７０４において、カウント「１」に応答してＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２により最初のビット（または、それに代えて２番目のビット）が出力される。このＳＴＢは、モジュロ２カウンタ６０２にもフィードバックされ、その結果、ＳＴＢがアサートされるとモジュロ２カウンタ６０２が１カウントをスキップし、次の２クロック・サイクルをロー（つまり両方をカウント「０」に）保持する。これによりステップ８０７において、デューティ・サイクル修正器６００は、ランダム・ビット・ソース２０２からのランダム・ビット・ストリーム内の次のビットを破棄する。この「次のビット」はラッチ３０４内にロードされているが、モジュロ２カウンタ６０２が次にアンド・ゲート３０９に対してカウント「１」を出力する前に、クロックされてラッチ３０６を通り抜けることからこれが可能になる。ステップ７０８においては、続くオーバーラップするペアとなるビットがランダム・ビット・ソース２０２から取り込まれ、その後プロセスがステップ７０２から繰り返される。このプロセスは、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。

【００３５】

デューティ・サイクル修正器６００の動作を別の形で図８に示す。最初のペアとなるビット（ビット０および１）の処理時においては、ペア内のビットが等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されな

い。それに加えて、ＳＴＢのアサートがないことからモジュロ２カウンタ６０２によるカウントのスキップも行なわれない。２番目のペアとなるビット（ビット２および３）はビット値が異なることから、デューティ・サイクル修正器６００が「０」を出力し、続いてモジュロ２カウンタ６０２がカウントをスキップすることから、その次のビット、つまりビット４が破棄される。３番目のペアとなるビット（ビット５および６）もビット値が等しくない。その結果、デューティ・サイクル修正器６００が「１」を出力し、モジュロ２カウンタ６０２がカウントをスキップすることから、その次のビット、つまりビット７が破棄される。最後のペアとなるビット（ビット８および９）は、ビット値が等しいことから破棄される。

【００３６】

ビット４および７を破棄することによって２番目のビットのペア（ビット２および３）と３番目のビットのペア（ビット５および６）の間の１次の自己相関、および３番目のビットのペアと４番目のビットのペア（ビット８および９）の間の１次の自己相関が低減される。修正後のビット・ストリームは、ランダム・ビット・ソース２０２によって出力された２番目のビットのペアと３番目のビットのペアの間、および３番目のビットのペアと４番目のビットのペアの間における２次の自己相関の影響を受けるが、その有意性はあまり高くない。

【００３７】

デューティ・サイクル修正器６００は、ランダム・ビット・ソースによって生成されたビットの間における１次の自己相関を低減する。しかしながら、それぞれの破棄されるビット（たとえば図８のビット４および７）がランダム・ビット・ストリーム内に一様に分布していないことから、修正後のビット・ストリームのデューティ・サイクルに非一様性が招かれる傾向を否定できない。

【００３８】

図９は、さらに別の実施形態、すなわちランダム・ビット・ソース２０２によって出力されるビットのペアの間における１次の自己相関の影響を軽減するデューティ・サイクル修正器９００を示している。デューティ・サイクル修正器９００は、ランダム・ビット・ソース２０２の、モジュロ５カウンタの特定のカウン

トに応じてシフトーインされたビットを破棄することによって、１次の自己相関を低減する。

【００３９】

デューティ・サイクル修正器９００は、デューティ・サイクル修正器３００に類似であるが、確認論理のトランスペアレント・ラッチ３０８が、モジュロ５カウンタ９０２、インバータ９０４、９０６、９０８、アンド・ゲート９１０、９１２、およびノア・ゲート９１４に置き換えられている点が異なる。モジュロ５カウンタ９０２は、３つのバイナリ出力ビットＣ０、Ｃ１、Ｃ２を有している。アンド・ゲート９１０は、３入力アンド・ゲートであり、第１の入力がインバータ９０４を介してＣ２に結合され、第２の入力がＣ１に結合され、第３の入力がインバータ９０８を介してＣ０に結合されている。アンド・ゲート９１２は、３入力アンド・ゲートであり、第１の入力がＣ２に結合され、第２の入力がインバータ９０６を介してＣ１に結合され、第３の入力がインバータ９０８を介してＣ０に結合されている。ノア・ゲート９１４は、アンド・ゲート９１０および９１２の出力を受け取り、アンド・ゲート３０９の一方の入力をドライブする。

【００４０】

デューティ・サイクル修正器９００の動作を図１０に示す。ステップ１０００およびモジュロ５カウンタ９０２のカウント「０」において、最初のビットがラッチ３０４にロードされる。カウント「０」と「１」については、信号ライン９１５上に信号がアサートされないことから、このビットは破棄される。ステップ１００２においては、カウント「１」と「２」に応答して、最初のペアとなるビットがランダム・ビット・ソース２０２からラッチ３０４および３０６にラッチされる。このラッチが、修正器１０００に最初のビットを破棄させる。ステップ１００４およびカウント「２」においては、エクスクルーシブーオア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ１００６において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ１００６においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力される

こともない。ステップ１００４およびカウント「２」において、２つのビットが互いに異なると判断されると、ステップ１００８においてＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２によりペア内の最初のビット（または、それに代えて２番目のビット）が出力される。

【００４１】

ステップ１０１０においては、カウント「３」および「４」に応答して、２番目のペアとなるビットがランダム・ビット・ソース２０２からラッチ３０４および３０６にラッチされる。ステップ１０１２およびカウント「４」においては、エクスクルーシブ－オア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ１０１４において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ１０１２およびカウント「４」において、２つのビットが互いに異なると判断されると、ステップ１０１６においてＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２によりペア内の最初のビット（または、それに代えて２番目のビット）が出力される。このプロセスが、ランダム・ビット・ソースから出力されるすべてのビットのペアに対する処理を完了するまで繰り返される。

【００４２】

図１１は、デューティ・サイクル修正器９００の動作をさらに別の形で示している。最初のビット、すなわちビット０は、修正器９００にロードされるが、最初のペアとなるビットがロードされるときに破棄される。最初のペアとなるビット（ビット１と２）は、ビット値が等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。２番目のペアとなるビット（ビット３と４）はビット値が異なることから、デューティ・サイクル修正器９００が「０」を出力する。その後、モジュロ５カウンタ９０２のカウントが「０」に戻り、その結果、ビット５が破棄される。３番目のペアとなるビット（ビット６と７）もビット値が異なり、デューティ・サイクル修正器９００は「１」を出力する。最後のペアとなるビット（ビット８および９）はビット値が互いに等しく、し

たがって破棄される。

【００４３】

ビット０と５を破棄することによって２番目のビットのペア（ビット３と４）と３番目のビットのペア（ビット６と７）の間の１次の自己相関が低減される。修正後のビット・ストリームは、２番目のビットのペアと３番目のビットのペアの間における２次の自己相関の影響を受けるが、その有意性はあまり高くない。カウント「０」（カウント「５」、カウント「１０」等）で破棄されるビットは、ランダム・ビット・ストリーム内に一様に分布し、それらを除外しても、結果的に修正後のビット・ストリームに関するデューティ・サイクルは概略で一様になる。

【００４４】

図１２は、さらに別の実施形態、すなわちランダム・ビット・ソース２０２によって出力されるビットのペアの間における１次の自己相関の影響を軽減するデューティ・サイクル修正器１２００を示している。デューティ・サイクル修正器１２００は、ランダム・ビット・ソース２０２が出力したビットから、比較されるビットのペアの間に挟まれるビットを破棄することによって１次の自己相関を抑える。

【００４５】

デューティ・サイクル修正器１２００は、デューティ・サイクル修正器３００に類似であるが、確認論理のトランスペアレント・ラッチ３０８が、カウント「２」のときにのみ信号ライン１２０４上に論理ハイの信号を出力するモジュロ３カウンタ１２０２に置き換えられている点が異なる。

【００４６】

デューティ・サイクル修正器１２００の動作を図１３に示す。ステップ１３００およびモジュロ３カウンタ９０２のカウント「０」において、最初のビットがラッチ３０４にロードされる。カウント「０」と「１」については、信号ライン１２０４上に信号がアサートされないことから、このビットは破棄されることになる。ステップ１３０２においては、カウント「１」と「２」に応答して、最初のペアとなるビットがランダム・ビット・ソース２０２からラッチ３０４および

３０６にラッチされる。このラッチによって、修正器１２００が最初のビットを破棄する。ステップ１３０４およびカウント「２」においては、エクスクルーシブーオア・ゲート３１０が、ペアを構成する２つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ１３０６において、ＡＣＣＥＰＴ（アクセプト）のアサートおよびＳＴＢのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ１３０６においては、いずれのビットもラッチ３１２によってラッチされることがなく、また信号ライン２１４に出力されることもない。ステップ１３０４およびカウント「２」において、２つのビットが互いに異なると判断されると、ステップ１３０８においてＡＣＣＥＰＴ（アクセプト）がアサートされ、ＳＴＢがアサートされて、ラッチ３１２によりペア内の最初のビット（または、それに代えて２番目のビット）が出力される。このプロセスが、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。

【００４７】

図１４は、デューティ・サイクル修正器１２００の動作をさらに別の形で示している。最初のビット、すなわちビット０は、修正器１２００にロードされるが、最初のビットのペアがロードされるとき破棄される。最初のペアとなるビット（ビット１と２）の処理時においては、ペア内のビットが等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。４番目のビット、すなわちビット３は、修正器１２００にロードされるが、２番目のペアとなるビットがロードされるとき破棄される。２番目のペアとなるビット（ビット４と５）はビット値が異なることから、修正器１２００が「０」を出力する。７番目のビット、すなわちビット６は、修正器１２００にロードされるが、３番目のペアとなるビットがロードされるとき破棄される。３番目のペアとなるビット（ビット７と８）はビット値が異なり、デューティ・サイクル修正器１２００は「１」を出力する。１０番目のビット、すなわちビット９は、修正器１２００にロードされるが、４番目のペアとなるビットがロードされるとき破棄される。４番目のペアとなるビット（ビット１０と１１）は、ビット値が等しいことから破棄される。

【００４８】

ビット０、３、６、９等を破棄することによって、比較を行うビットのペアの間における１次の自己相関が低減される。修正後のビット・ストリームは、比較を行うビットのペアの間における２次の自己相関の影響を受けるが、その有意性はあまり高くない。モジュロ３カウンタ１２０２のカウント０、３、６、９等において破棄されるビットは、ランダム・ビット・ストリーム内に一様に分布し、それらを除外しても、結果的に修正後のビット・ストリームに関するデューティ・サイクルは概略で一様になる。

【００４９】

以上、ランダム・ビット・ソースのランダム・ビット・ストリーム内の連続する２つのビットを比較するものとしてデューティ・サイクル修正器の説明を行ってきたが、変形実施形態として、連続しないビットを比較することもできる。たとえば、ストレージ回路２０４と２０６の間に追加のストレージ回路を挿入し、あるいはそれぞれのストレージ回路を異なるクロックもしくは異なるクロック・エッジを用いてクロックすることが考えられる。

【００５０】

また、ここで説明した出力回路２１２は、ストレージ回路２０４と２０６のうちのいずれか一方の出力を受け取る。変形実施形態においては、比較論理２０８に、ストレージ回路２０４と２０６にストアされているデータに応答して出力回路２１２に提供されるデータを決定する論理を含めることができる。

【００５１】

ランダム・ビット・ソースから実質的に一様な「１」と「０」の分布を生成するための、ここで説明したデューティ・サイクル修正器は、コンピュータ・ネットワークを介して送られるメッセージの符号化および復号化を行うための乱数発生器と組み合わせて使用することができる。図１５は、上記のいずれかの実施形態を使用して暗号化されたメッセージを送信するためのコンピュータ・ネットワークを示したブロック図である。ネットワーク１５００は、送信ホスト・コンピュータ１５０２およびネットワークを介してそれに結合された受信ホスト・コンピュータ１５０４を含んでいる。送信ホスト・コンピュータおよび受信ホスト・

コンピュータは、ともにネットワーク・インターフェース・デバイスを備え、それによってホスト・コンピュータ・システムとネットワーク・メディアの間の物理的かつ論理的な接続が提供される。さらにいずれのホスト・コンピュータにも暗号化回路／解読回路が備わり、それが、データ通信のセキュリティに関する各種の暗号機能を実行する。送信ホスト１５０２は、暗号化回路／解読回路１５０６を備えており、受信ホスト１５０４は、暗号化回路／解読回路１５０７を備えている。暗号化回路／解読回路１５０６および１５０７には、それぞれ乱数発生器１５０８および１５０９が備わり、そこには、図２、３、６、９、または１２に示した実施形態のいずれかが採用されている。これらの乱数発生器は、公開キー／秘密キーシステムにおける公開キー／秘密キーの生成に使用される。

【００５２】

ネットワーク１５００においては、送信ホスト１５０２と受信ホスト１５０４の間の安全な通信を保証するために、各種のデータ暗号化方法を使用することができる。一実施形態においては、ネットワーク１５００が公開キー（非対称）暗号システムを使用する。公開キーシステムにおいては、２つの異なるキーが使用される。一方のキーは、送信側がメッセージの符号化のために使用し、他方のキーは、受信側が符号化されたメッセージの復号化のために使用する。このシステムにおいては、暗号化（公開）キーは広く公開してもよいが、復号（秘密）キーは、意図された受信側だけがメッセージの復号化を行えるように秘密にする必要がある。公開キーおよび秘密キーは、通常、非常に大きな素数および乱数からともに導かれる。したがって、真にランダムなキーのペアを生成するためには、効果的な乱数発生器が必要になる。

【００５３】

公開キーシステムを使用するデータ送信の例において、送信ホスト１５０２は、受信ホスト１５０４に送信するためのメッセージＭを作成する。この伝送のために使用される２つのキーは、受信側の公開キー（PuK_R）および受信側の秘密キー（PrK_R）からなる。通常、受信側は、公に入手可能な登録キーから公開キーを選択し、受信側のみが知っている変換プロセスを介して、当該公開キーから秘密キーを導く。つまり、一般に公開キーと秘密キーの間の相関は、秘密で

あり、かつ安全である。送信ホスト１５０２は、公開キーを使用し、暗号化回路／解読回路１５０６を介してメッセージを符号化し、符号化済みのメッセージM’を生成する。符号化が行なわれた後は、適切な秘密キーを使用しない限りメッセージを復号化することができない。受信ホスト１５０４は、メッセージを受信すると、秘密キーを用いてメッセージM’の復号化を行い、オリジナルのメッセージMを取り出す。

【００５４】

一実施形態においては、受信ホスト１５０４内の暗号化回路／解読回路１５０７が、図２、３、６、９、または１２の実施形態のいずれかを採用した乱数発生器１５０９を備えている。このテクニックは、乱数発生器１５０９からのビットの分布が充分に一様かつランダムであり、そのため公開キーと、受信ホスト１５０４によって生成される秘密キーの間に一貫性のある相関が存在しない。ネットワーク１５００内に示されるように、送信ホスト１５０２内の暗号化回路／解読回路１５０６もまた、図２、３、６、９、または１２の実施形態のいずれかを採用した乱数発生器１５０８を備えている。これにより送信ホスト１５０２は、公開キーによる送信を採用するときの、安全な秘密キーおよび公開キーの生成が可能になる。これらのキーのペアの生成には、秘密キーの網羅的でないサーチが極めて困難になるように高度のランダム性が要求される。

【００５５】

別の実施形態においては、ネットワーク１５００が単一キー（対称）システムを使用して、暗号機能を実行する。単一キーシステムの場合には、送信側と受信側が１つのキーを共有し、それを使用して送信側はメッセージの暗号化を行い、受信側は、符号化されたメッセージの解読をおこなう。このシステムの信頼性は、キーのセキュリティに依存する。したがって、第三者に知られることのない、送信側と受信側の間のみにおけるキーの開示のために安全なプロセスが必要になる。この実施形態においては、通常、メッセージ・トランザクションが異なるごとに異なるキーが使用される。つまり、各種のキーが生成されることから、あるメッセージ・トランザクションに使用されるキーが、別のメッセージ・トランザクションに使用されたキーから決定不可能であることが保証される必要がある。

このシステムの場合、ネットワーク１５００の各ホスト・コンピュータ内の暗号化回路／解読回路において、乱数発生器が使用されてホスト・コンピュータ間で送信されるメッセージ・データの符号化および復号化を行うためのランダムなキーパターンが生成される。

【００５６】

なお、ここでは単一キーおよび公開キー／秘密キー暗号システムとの関連から本発明の実施形態を説明したが、本発明の実施形態は、安全なコンピュータ・ネットワーキングのための、これ以外のタイプの暗号システムにも使用できることに注意する必要がある。さらに、図１５に示した暗号化回路／解読回路は、安全なデータ送信システムにおけるメッセージの符号化および復号化、送信されたメッセージの認証、ディジタル署名の検証、およびその他の機能を含めた各種の暗号機能の実行に使用することができる。

【００５７】

以上のとおり、一様なデューティ・サイクルの乱数発生器を作るための回路について説明した。ここでは、特定の具体例とする実施形態を参照して本発明についての説明を行ったが、特許請求の範囲に示される本発明の精神ならびに範囲はそれよりも広く、それから逸脱することなくこれらの実施形態に対して各種の修正ないしは変更を加え得ることは明らかである。したがって、明細書ならびに図面は、限定の意味ではなく例示と考える必要がある。

【図面の簡単な説明】

【図１】

リニア・フィードバック・シフト・レジスタを使用する従来の乱数発生器を示した図である。

【図２】

ランダム・ビット・ソースおよびデューティ・サイクル修正器の一実施形態を示したブロック図である。

【図３】

図２に示したデューティ・サイクル修正器の一実施形態を示した論理図である。

【図４】
図２に示したデューティ・サイクル修正器の動作を示したフローチャートである。
【図５】
図３に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。
【図６】
図２に示したデューティ・サイクル修正器の別の実施形態を示した論理図である。
【図７】
図６に示したデューティ・サイクル修正器の動作を示したフローチャートである。
【図８】
図６に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。
【図９】
図２に示したデューティ・サイクル修正器の一実施形態を示した論理図である。
【図１０】
図１０に示したデューティ・サイクル修正器の動作を示したフローチャートである。
【図１１】
図９に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。
【図１２】
図２に示したデューティ・サイクル修正器の一実施形態を示した論理図である。
【図１３】
図１２に示したデューティ・サイクル修正器の動作を示したフローチャートで

ある。

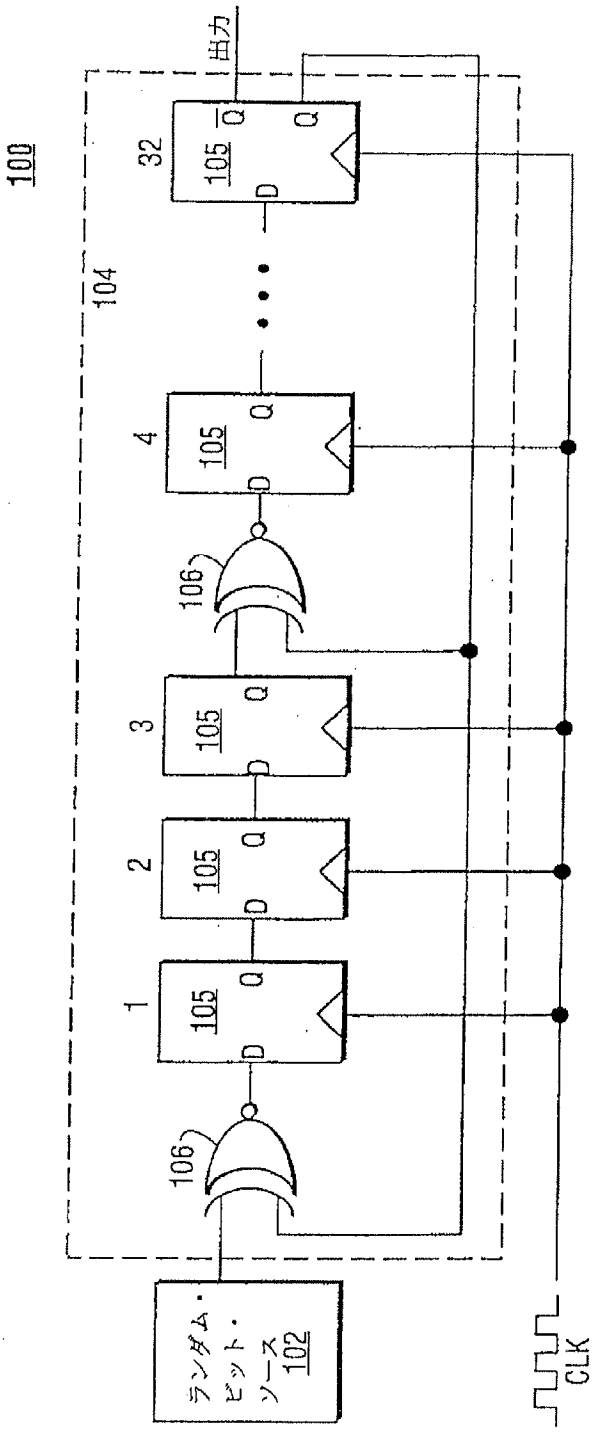
【図１４】

図１２に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

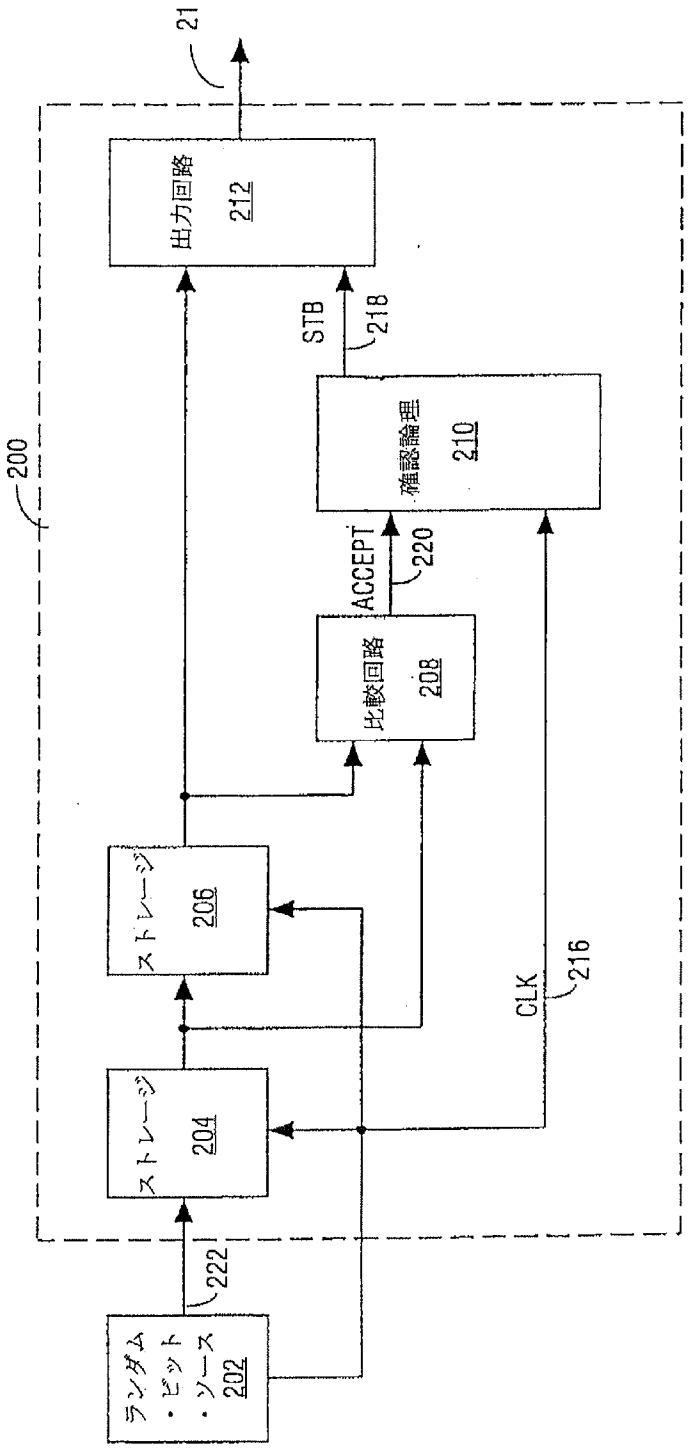
【図１５】

本発明の一実施形態に従ったデータ暗号化／解読のためのビット・ペアリング・システムを使用するコンピュータ・ネットワークを示したブロック図である。

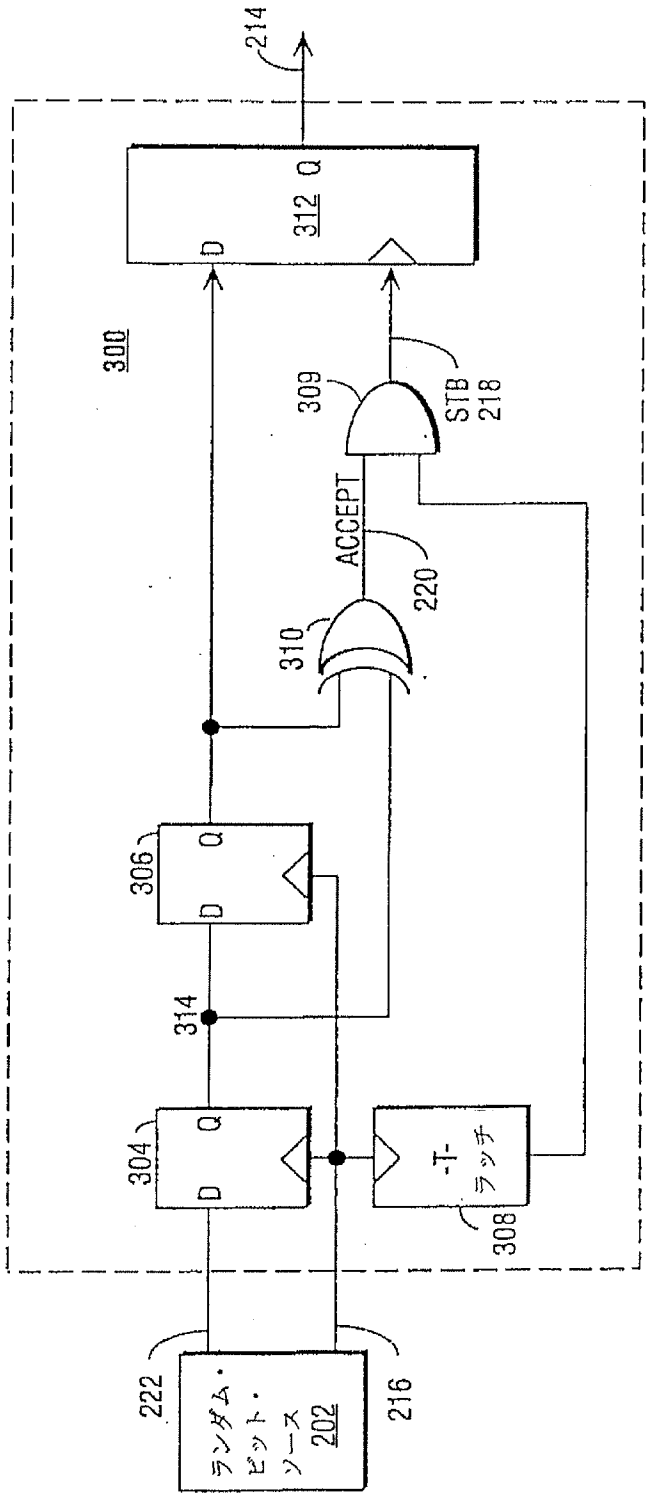
【図１】



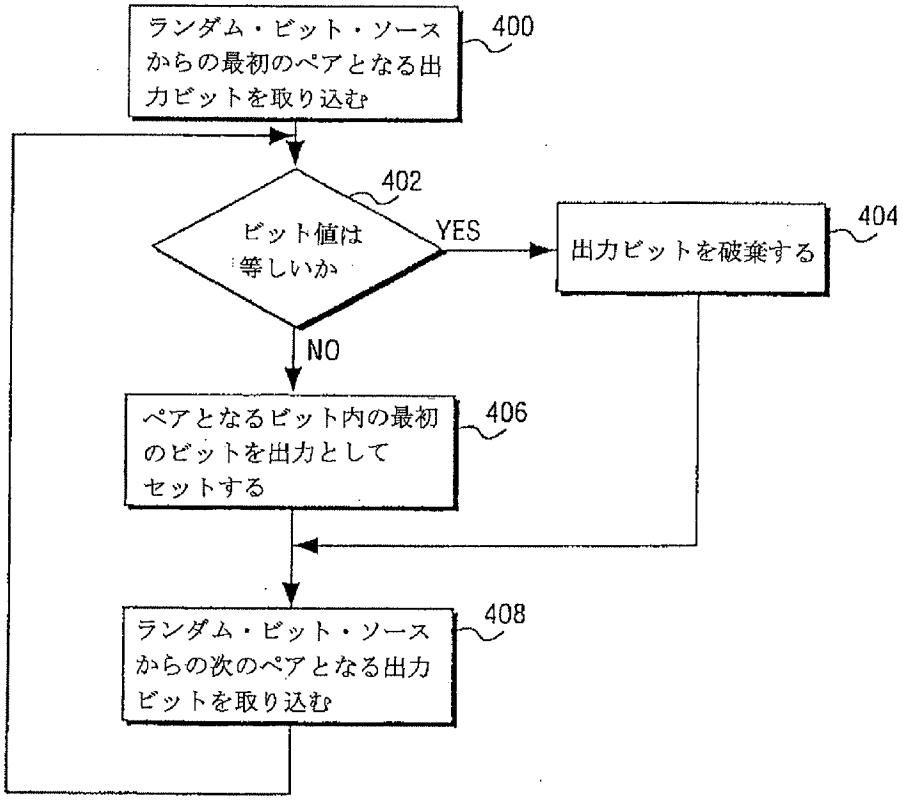
【図２】


21
200
出力回路
212
STB
218
確認論理
210
ACCEPT
220
比較回路
208
ストレージ
206
ストレージ
204
CLK
216
ランダム
・ビット
・ソース
202
222

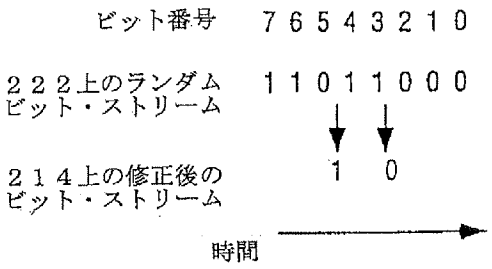
【図３】


214
312
Q
D
300
309
STB
218
ACCEPT
220
310
306
Q
D
314
304
Q
D
-T-
ラッチ
308
222
ランダム・
ビット・
ソース
202
216

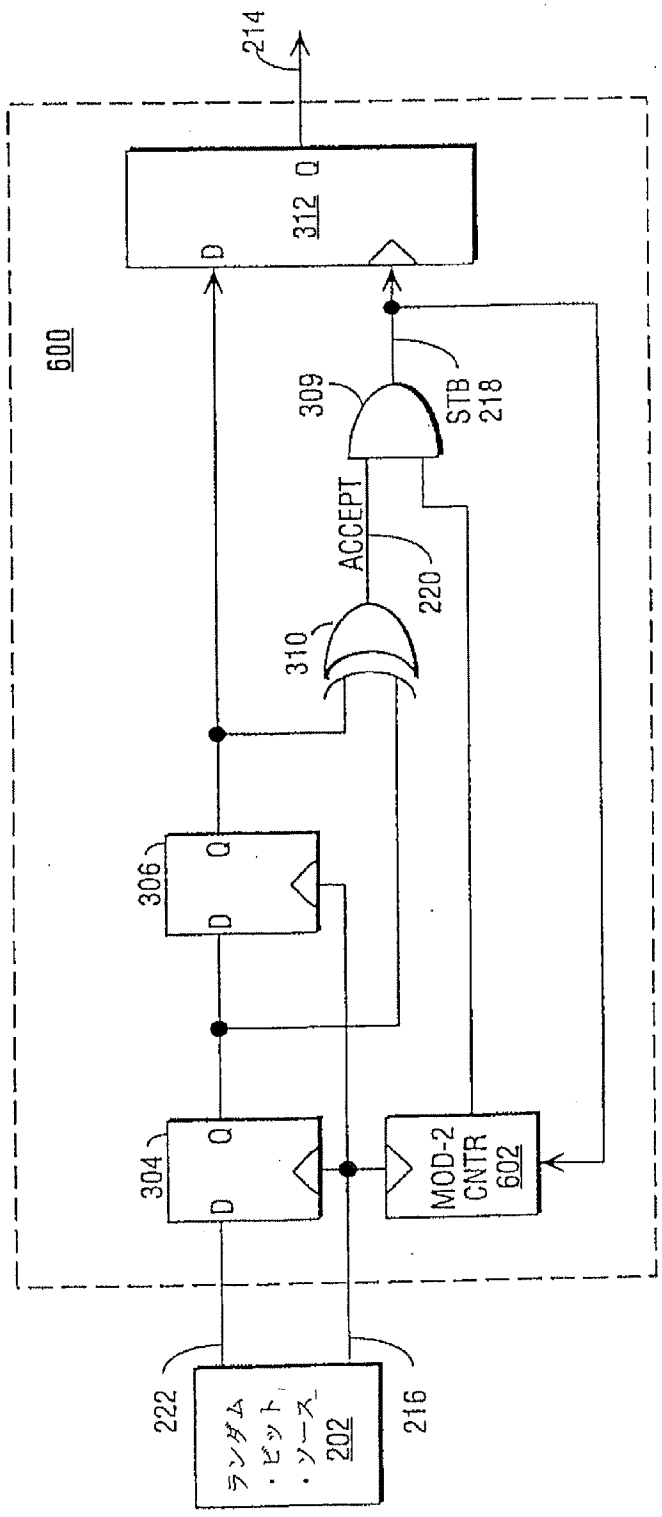
【図４】


ランダム・ビット・ソースからの最初のペアとなる出力ビットを取り込む
400
402
ビット値は等しいか
YES
出力ビットを破棄する
404
NO
ペアとなるビット内の最初のビットを出力としてセットする
406
ランダム・ビット・ソースからの次のペアとなる出力ビットを取り込む
408

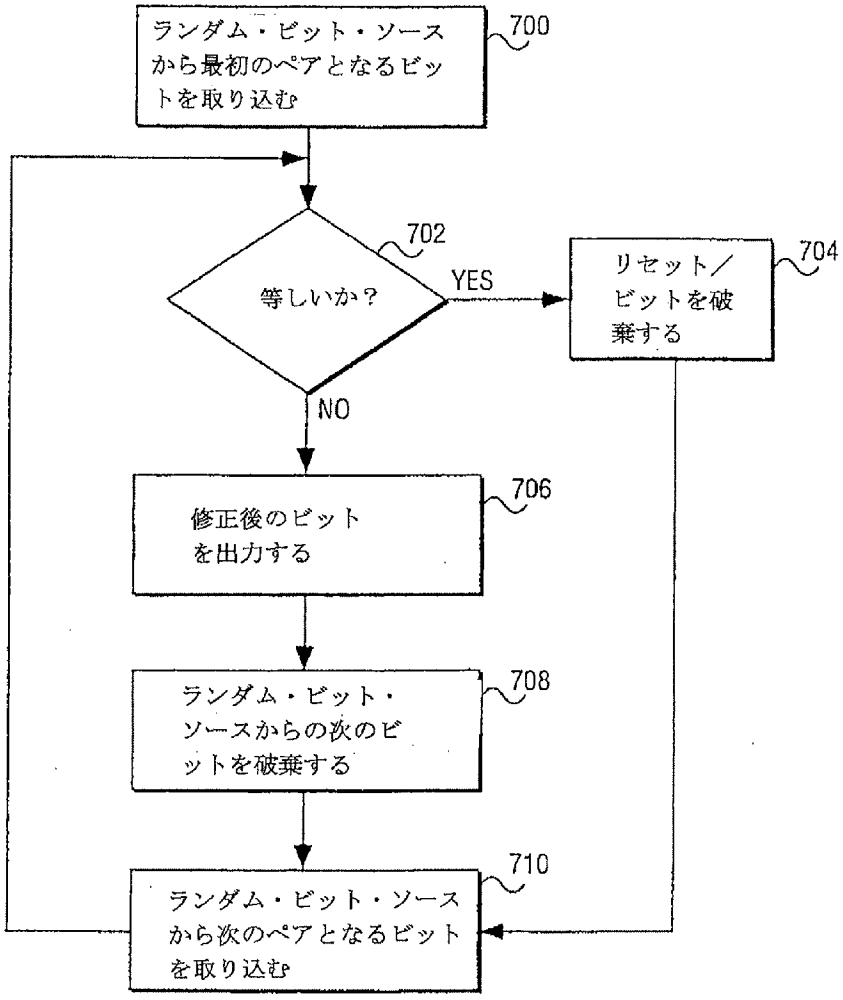
【図５】


ビット番号
7 6 5 4 3 2 1 0
２２２上のランダムビット・ストリーム
1 1 0 1 1 0 0 0
２１４上の修正後のビット・ストリーム
1 0
時間

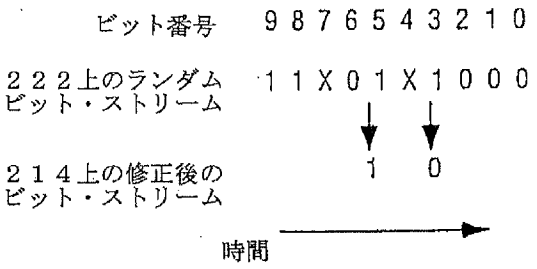
【図６】


214
600
312
D
Q
309
STB
218
ACCEPT
220
310
306
304
MOD-2
CNTR
602
222
ランダム
・ビット
・ソース
202
216

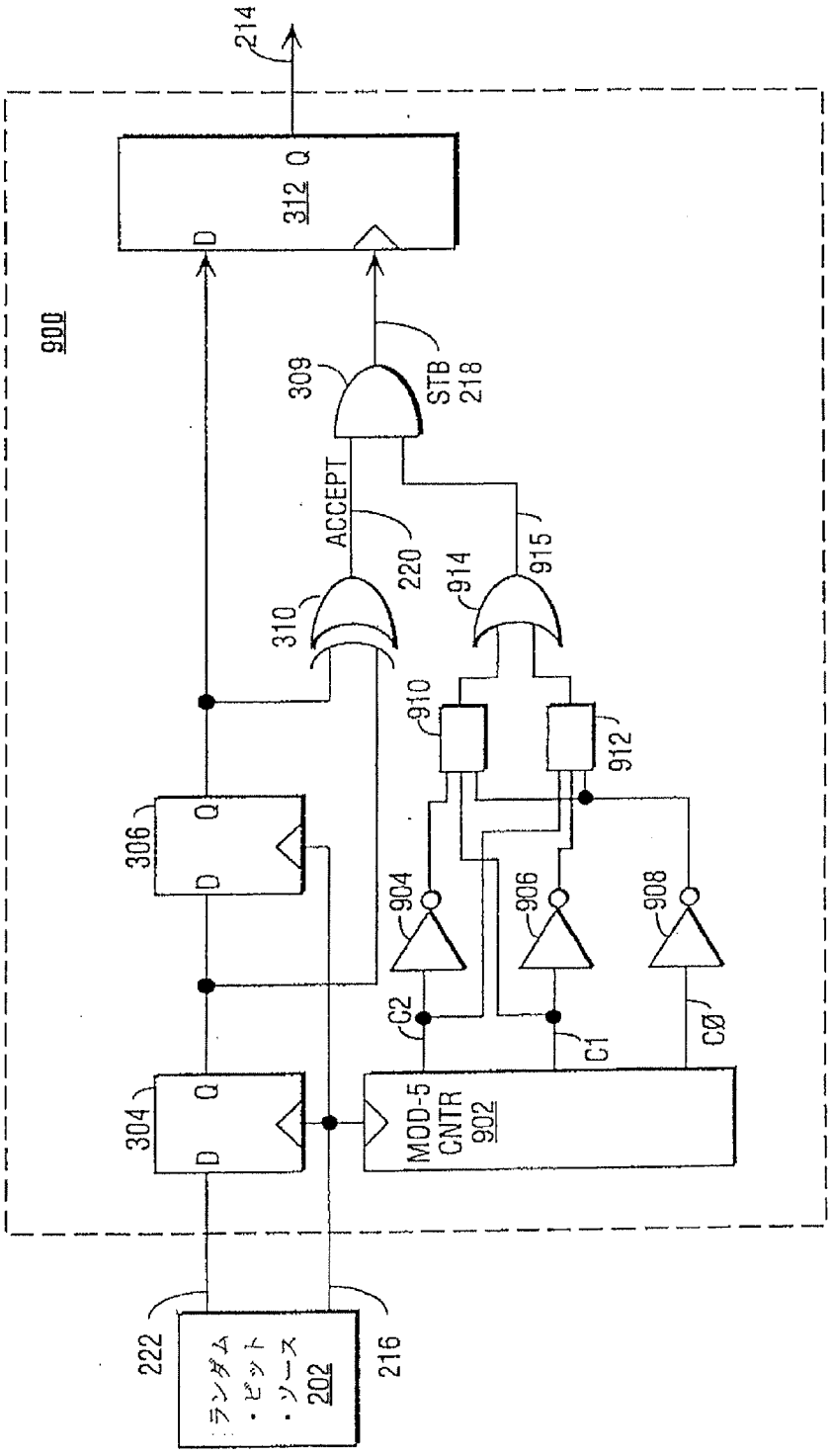
【図７】


ランダム・ビット・ソースから最初のペアとなるビットを取り込む
700
等しいか？
702
YES
NO
リセット／ビットを破棄する
704
修正後のビットを出力する
706
ランダム・ビット・ソースからの次のビットを破棄する
708
ランダム・ビット・ソースから次のペアとなるビットを取り込む
710

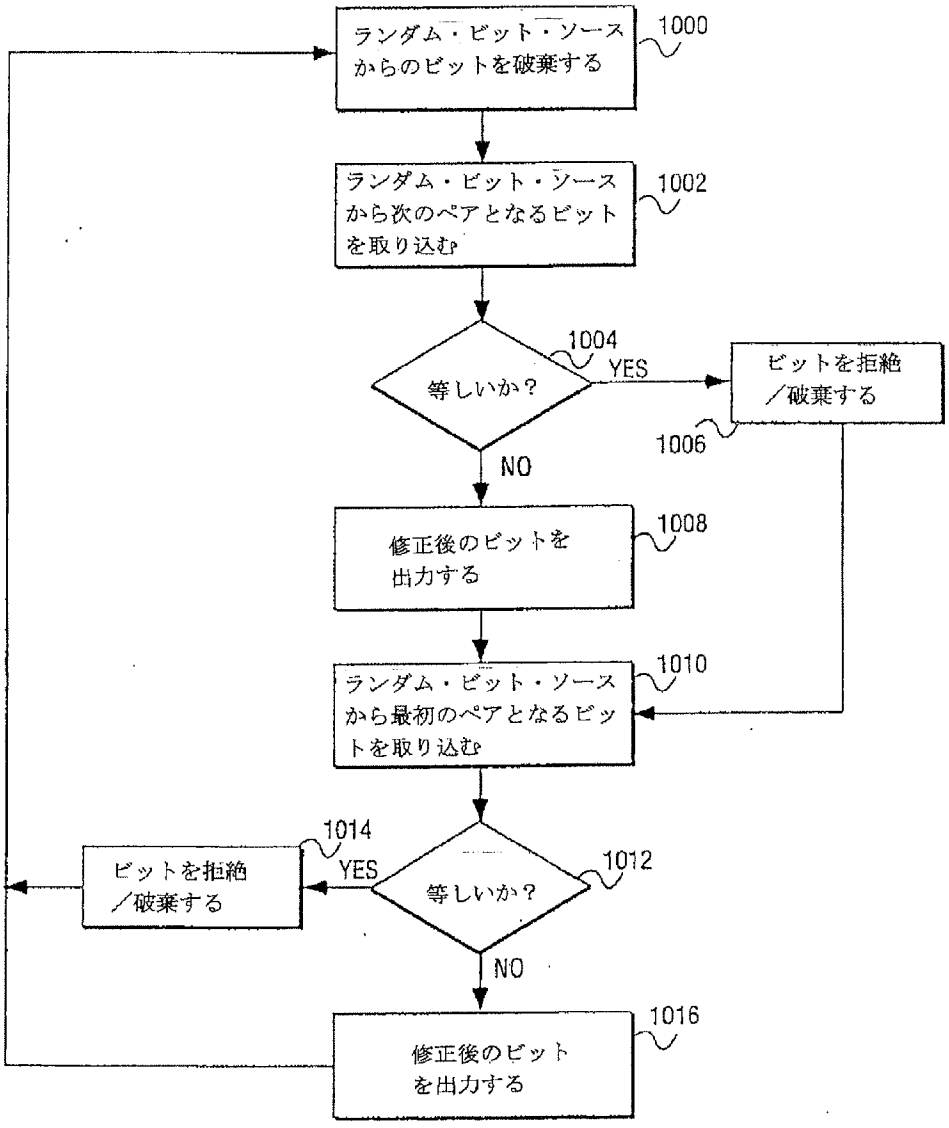
【図８】


ビット番号 9 8 7 6 5 4 3 2 1 0
２２２上のランダムビット・ストリーム 1 1 X 0 1 X 1 0 0 0
２１４上の修正後のビット・ストリーム 1 0
時間

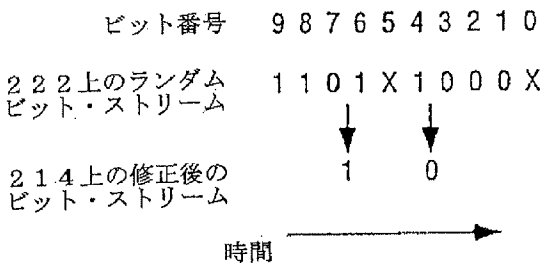
【図９】


214
900
312 Q
D
309
STB
218
ACCEPT
220
310
914
915
910
912
306
304
904
906
908
C2
C1
C0
MOD-5
CNTR
902
222
216
ランダム
・ビット
・ソース
202

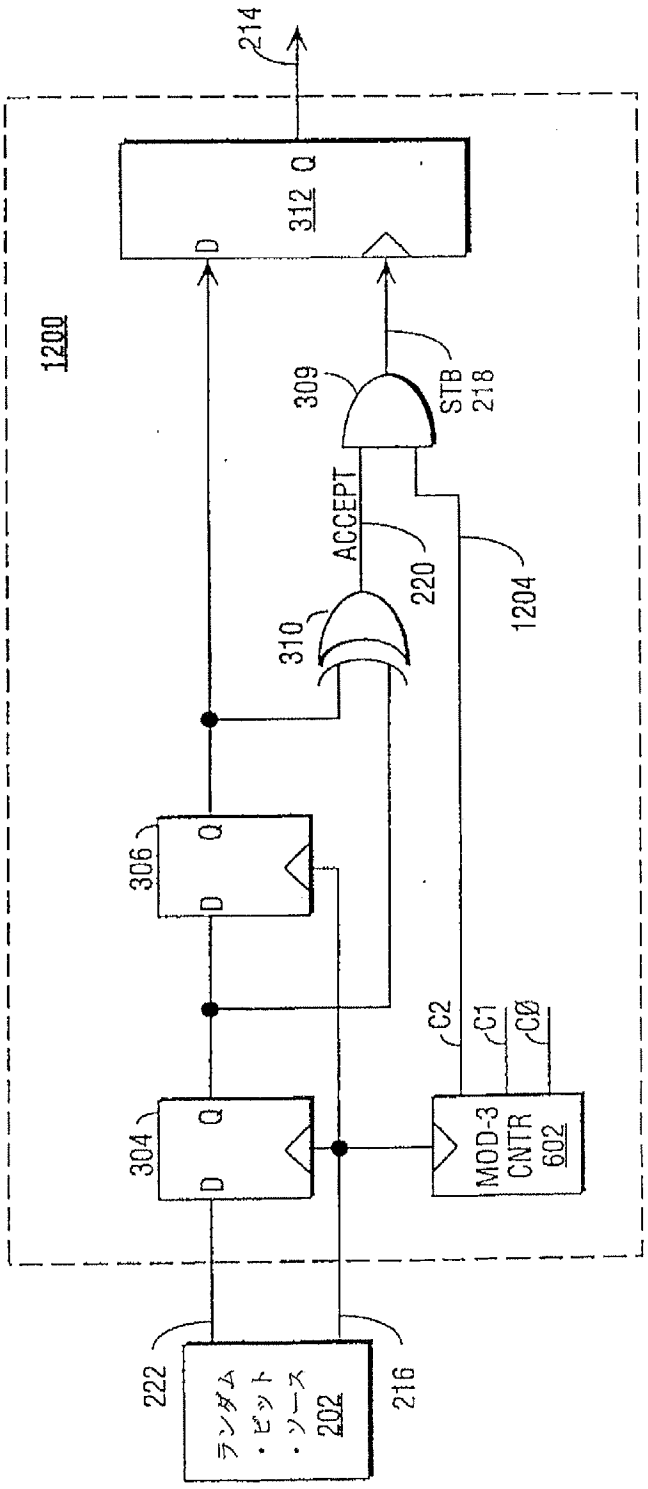
【図１０】


ランダム・ビット・ソースからのビットを破棄する
1000
ランダム・ビット・ソースから次のペアとなるビットを取り込む
1002
等しいか？
1004
YES
ビットを拒絶／破棄する
1006
NO
修正後のビットを出力する
1008
ランダム・ビット・ソースから最初のペアとなるビットを取り込む
1010
等しいか？
1012
YES
ビットを拒絶／破棄する
1014
NO
修正後のビットを出力する
1016

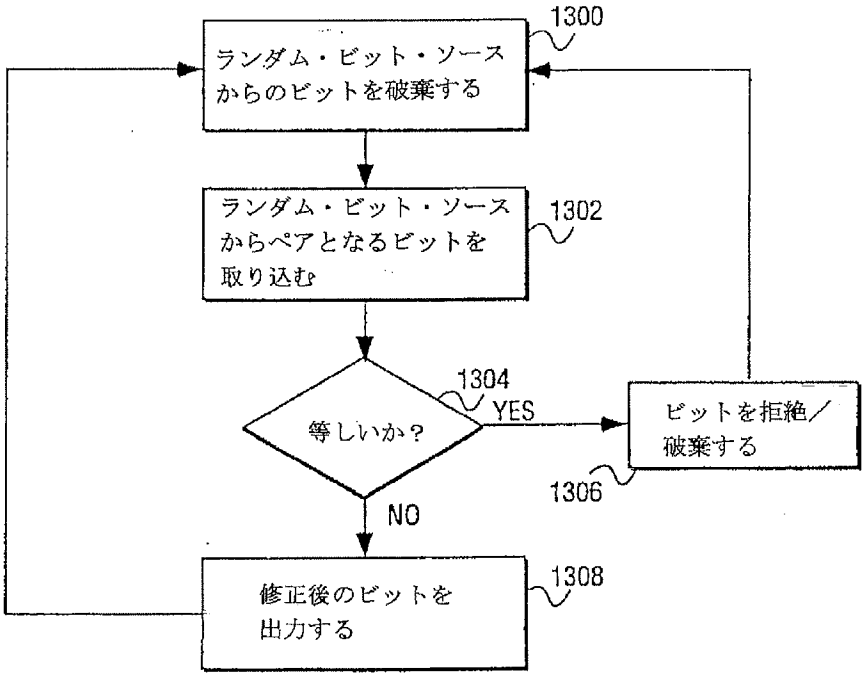
【図１１】


ビット番号 9 8 7 6 5 4 3 2 1 0
２２２上のランダムビット・ストリーム 1 1 0 1 X 1 0 0 0 X
２１４上の修正後のビット・ストリーム 1 0
時間

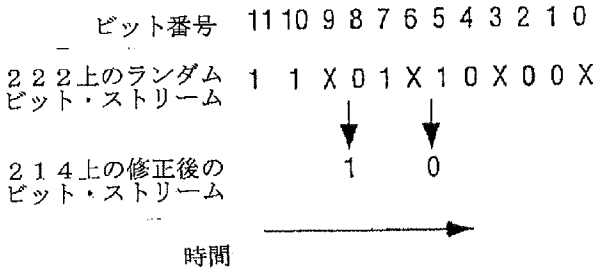
【図１２】


214
312
Q
D
1200
309
STB
218
ACCEPT
220
1204
310
306
Q
D
C2
C1
C0
304
Q
D
MOD-3
CNTR
602
222
ランダム
・ビット
・ソース
202
216

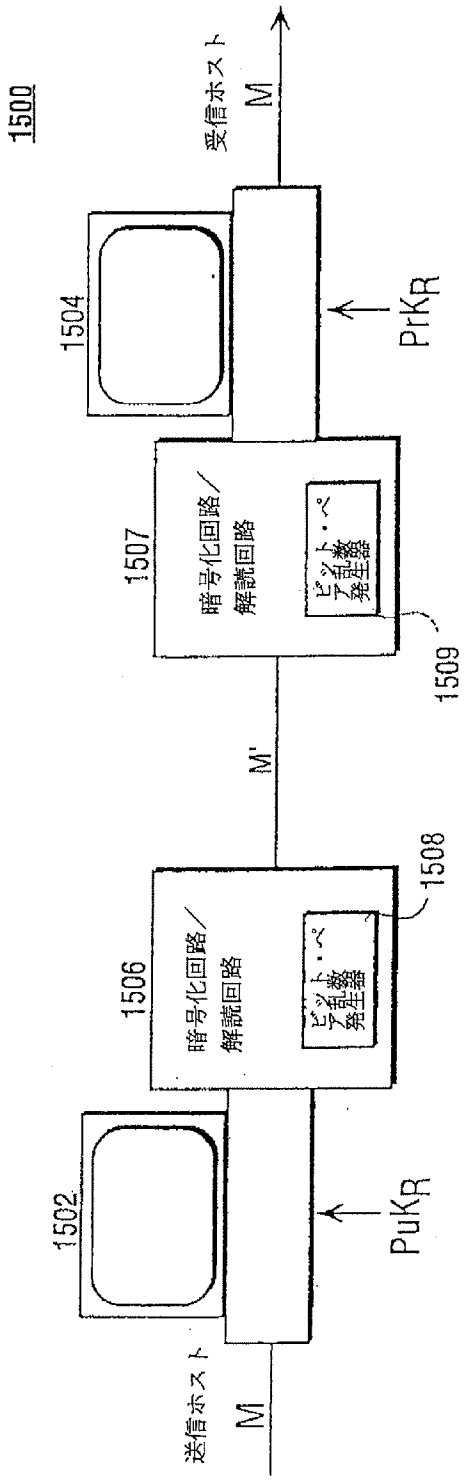
【図１３】


1300
ランダム・ビット・ソース
からのビットを破棄する
ランダム・ビット・ソース
からペアとなるビットを
取り込む
1302
1304
等しいか？
YES
ビットを拒絶／
破棄する
1306
NO
修正後のビットを
出力する
1308

【図１４】


ビット番号 11 10 9 8 7 6 5 4 3 2 1 0
２２２上のランダム
ビット・ストリーム
1 1 X 0 1 X 1 0 X 0 0 X
２１４上の修正後の
ビット・ストリーム
1 0
時間

【図１５】


1500
送信ホスト
M
1502
PuKR
1506
暗号化回路／
解読回路
ビット・ベア乱数発生器
1508
M'
1507
暗号化回路／
解読回路
ビット・ベア乱数発生器
1509
1504
PrKR
受信ホスト
M

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 00/06916

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 844 925 A (DENT PAUL W) 1 December 1998 (1998-12-01) abstract column 3, line 43 -column 4, line 32 column 5, line 12 - line 41 claim 1 figure 3 ---	1,2,4-8, 10,17
A	DE 40 06 251 C (WOLFGANG BITZER) 11 April 1991 (1991-04-11) abstract column 1, line 3 - line 35 column 2, line 16 - line 50 figure 3 --- -/--	1,2,10

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 September 2000	21/09/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

INTERNATIONAL SEARCH REPORT

Inter ional Application No
PCT/US 00/06916

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 781 458 A (GILLEY JAMES E) 14 July 1998 (1998-07-14) abstract column 2, line 63 -column 3, line 12 column 5, line 19 - line 43 figures 3,4	1,10,17

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/US 00/06916

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5844925 A	01-12-1998	AU 718539 B	13-04-2000
		AU 3959597 A	09-02-1998
		CA 2258362 A	22-01-1998
		CN 1225769 A	11-08-1999
		EP 0913040 A	06-05-1999
		WO 9802990 A	22-01-1998
DE 4006251 C	11-04-1991	NONE	
US 5781458 A	14-07-1998	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国　　EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW